USAWC STRATEGY RESEARCH PROJECT

INFORMATION TECHNOLOGY: WHEN IS ENOUGH?

by

Colonel Darin Talkington
United States Army

Dr. J. Boone Bartholomees
Project Adviser

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
30 MAR 2007	**Strategy Research Project**	**00-00-2006 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Technology When is Enough?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Darin Talkington	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**18**	

ABSTRACT

AUTHOR: Colonel Darin Talkington

TITLE: Information Technology: When Is Enough?

FORMAT: Strategy Research Project

DATE: 22 March 2007 WORD COUNT: 5559 PAGES: 18

KEY TERMS: Information Overload, Battlefield Information

CLASSIFICATION: Unclassified

When does one have enough information technology? When do we cross the point of diminishing return? At what point in time do information planners and program managers provide too much information access? Will the vast Army investments in information technology, high speed data networking, and robust beyond line-of-sight telecommunications at the brigade and below level enable the tactical war fight? Or, will this investment in technology at the tactical level overtax already weary staffs and further inhibit their ability to focus their commanders on the most relevant information necessary to make sound timely decisions? As part of this research I plan to present an understanding of the challenges currently facing tactical commanders with regard to information overload. I will provide examples that underscore the dangers inherent in tactical commanders having too much information or too much reliance on information technology. I will present the current year range of investments being made in information technology and attempt to present the merits of increased investment in information analysis and dissemination management. I will compare the capabilities of information technology enablers like tactical networking support against the anticipated threats over the upcoming decade.

INFORMATION TECHNOLOGY: WHEN IS ENOUGH?

> The U.S. Army and the commercial sector are very much engaged in new and emerging technologies, and the service is extending the edge of the network. In the past, the Army network went to the tactical brigades through mobile subscriber equipment…the Army will be extending the network down to the battalion level. And, now the information technology network reaches in some cases down to the platform—the soldier and/or the weapon.
>
> —Lt. Gen. Steven W. Boutelle
> Chief Information Officer/G-6

This paper addresses a difficult and persistent problem. When does one have enough information technology? When do we cross the point of diminishing return? When do information planners and program managers provide too much information access.

The author has been a Signal Officer in the United States Army for more than twenty years. Over the span of that time and at every level from Company through Army headquarters, I have been a party to attempts to meet ever increasing demands that senior leaders put on planning, programming, procuring and installing the newest information technology gadgets as a means to achieve increased levels of effectiveness, efficiency and/or productivity. Though we had limited means to effectively measure increases in productivity, in most cases the infusion of technology failed to achieve the levels of effectiveness anticipated or desired. At best the technology provided a means to organize information for presentation or layout all the raw data that underscored the complexity of the environment.

Will the vast Army investments in information technology, high speed data networking, and robust beyond line-of-sight telecommunications at the brigade and below level enable the tactical war fight? Or, will this investment and implementation of technology at the tactical level overtax already weary staffs and further inhibit their ability to focus their commanders on the most relevant information necessary to make sound, timely decisions? The United States Army has undertaken multi-billion dollar investments in building robust tactical communications infrastructure/connectivity down to the very lowest level. These programs include such information system enablers as the Joint Network Node (JNN), Warfighter Information Network—Tactical (WIN-T), Battle Command on-The-Move (BCOTM), and Joint Tactical Radio Systems (JTRS) to name a few. Has sufficient investment been made in conditioning (training and disciplining) tactical staffs in the necessary processes to effectively utilize and manage these technologies as they are infused?

Capabilities under development include the ability to download real time full video from multiple sources to multiple platforms simultaneously while traveling along rough terrain at 30+ miles an hour. This sounds very attractive in the technical sense, however, how much thought has been given to the resources necessary to actually analyze the vast amounts of input from these video and/or electronic sensors? Is the analytical capability that is resident at the brigade and below level equal to this task? Should a robust analytical capability reside at the brigade or below level or should they (the brigade and below staffs) simply be the recipients of already processed and analyzed intelligence?

As part of this research I will present an understanding of the challenges currently being faced by tactical commanders and their staffs with regard to information overload. I will provide examples that underscore the dangers inherent in tactical commanders having too much information and too much reliance on information technology. I will present the current year range of investments being made in information technology and attempt to present the merits of increased investment in information analysis and dissemination management. I will compare the capabilities of information technology enablers like tactical networking support against the anticipated threats over the upcoming decade in an era when we face emerging asymmetric adversaries. Though I cannot definitively answer how much information is too much at the different levels of tactical command, I will present research that indicates that there are limits to the amount of information individuals can effectively process.

Have we put our tactical leaders at a disadvantage by increasing their dependence on technology when conducting their close fight? Before I begin outlining some of my concerns about this broad deployment of information technology to all levels in the Army, let me express my views about the positive aspects of technology.

The development of computer technology and wireless communications has brought great changes to the world. There is scarcely a point on the globe that has not been touched by this revolution in information age technology. Instant communications are possible via the internet protocol (IP) based packet routing, which makes communications across the globe subjectively as easy and as cheap as communications across the street. News video is broadcast in real-time, around the clock. Instead of waiting for weeks, days, or even hours to learn of critical events, today it is possible to actually observe critical events unfolding on a distant continent.[1]

Dangers arising from this near simultaneous reporting of events around the world has caused information agencies to short circuit the process by which information is confirmed or thoroughly investigated prior to broadcast. Information is power, and 24-hour reporting means that news agencies that report first gain an advantage on their competitors. The audience, be it

military or otherwise, falls prey to misleading or incomplete information associated with this focus on getting the story out fast.

Powerful new tools now serve the modern military commander. Satellite imagery lets him see the ground occupied by his enemy and informs him of the conditions to a fine degree of accuracy. Signals intelligence and other sources inform him of potential enemy intentions. Position locating and reporting equipment displays the locations of subordinate elements on the move and at rest. Instant communications down to the very lowest level, even to the individual soldier if need be, give the commander the ability to personally involve himself from a distance in any segment of any military operation he chooses. The commander can virtually see any part of the complex whole. To a great extent, communications no longer limit a commander's ability to directly manage or control any piece of any military action, no matter how small. The communications network covers the world of military operations "from the foxhole to the White House." Infrastructure is the true network, technically non-hierarchical and ideally seamless.[2]

> New tools and processes of waging war like information warfare (IW), network-centric-warfare (NCW), integrated command and control (C4ISR), systems of systems, all powered by information technology, have led to a revolution in military affairs (RMA). Armed forces the world over are facing a paradoxical situation where they need to accomplish more with less. The tasks are increasing, while the resources and manpower are decreasing.[3]

The efficiencies garnered by information technology was used by the United States Department of Defense back in the early 1990 when the military was being reshaped after the fall of the Soviet Union. Likewise, one of the key tenets by which DoD transformation was to occur within the last six years was through the inherent benefits that information technology would provide. This necessitates working smarter and looking for force multipliers. Network-centric warfare, which was a term first developed in the late 1990s, was intended as an enabler to manage this paradox.[4]

Network-centric-warfare represents a fundamental shift from what we call platform-centric warfare to a network-centric environment. Though we have traveled some distance since this new concept was first presented in the late 1990's, we still do not fully understand its implications. In fact, as recently as 2005, there was still no universally accepted definition or understanding of what exactly network-centric warfare is or is not. There has yet to emerge any theorist the likes of Carl von Clausewitz or Sun Tzu to develop information warfare theory.

> However, we can gain some insight through the general observation that nations make war the same way they make wealth. As example, these technologies, combined with high-volume, high-speed data access and technologies for high speed networking have led to the emergence of network-centric computing. Information "content" can now be created, distributed, and easily exploited across

> the extremely heterogeneous global environment. Networking in stock markets has led to a shift from trader-centric systems to network-centric systems. This has considerably reduced the time taken to complete transactions, and it has increased customer awareness about prices of stocks and shares. Similarly, a shift to network-centric operations will help the military improve resource tracking and logistics management.[5]

IT investments in today's military are primarily about speeding up the decision cycle or getting inside the adversaries decision cycle.

> A basic element of military activity on the battlefield is the Observe-Orient-Decide-Act (OODA) loop. The information part of this cycle (or OODA loop) is carried out by sensors and associated systems responsible for generation of information. This activity is followed by decision and action in the cyclical fashion until the specific action is completed. An activity may require more than one cycle for completion or a number of cycles before the actions reach finality. The structure or model for network-centric warfare is designed to compress the time taken to complete the OODA loop.[6]

The cost of achieving this level of compressed response times and sophistication is the cost of providing a high-performance information grid in the austere battlefield environment. Assured, redundant, high-speed, networks spanning thousands of square miles on varieties of terrain and extreme environmental conditions are a pre-requisite for this level of service. The pace of future battle will be so swift that there will be no time to constantly refer to higher headquarters for instructions and advice. A typical military hierarchical structure in such an environment will fail. Therefore, future tactical commanders will need the same view of the battlefield as do their superior headquarters. Commanders will have to decentralize and delegate, while officers on the battlefront will have to be fully aware of the disposition of forces, status of supply, location of adjacent units, changes to the rules of engagement and/or the evolving political factors so that they can make quick, informed decisions.[7]

Network-centric-warfare enables a shift from attrition-style warfare to a much faster and more effective warfighting style characterized by the new concepts of speed of command and self-synchronization. It allows for an understanding of all elements of battle space and battle time. Operationally it provides a close linkage between the units and the operating environment, and tactically it provides speed. It is one of the most important rationales for this being considered a revolution in military affairs.[8] In the last decade, there has been a proliferation of articles, books and references on the information revolution and the RMA. Futurists like Alvin and Heidi Toffler, John Naisbitt and others gave early indications of this revolution they envisioned happening. The Gulf War, fall of the Soviet Union, war in Yugoslavia

and technological development in the civilian IT industry have increased interest and investment in this emerging capability.[9]

In the early 1990s senior Army leaders began reading emerging thought on information systems technology and studying ways to leverage technology's benefits against the force changes anticipated as paying the peace dividend. With an understanding of these benefits the Army is transforming and modernizing while maintaining its high operational tempo. These irregular, catastrophic and disruptive challenges are likely to continue, along with more traditional military challenges. To maintain the highest quality force, the Army is pursuing initiatives to produce and sustain a full spectrum of capabilities to defend the homeland, sustain the long war, conduct irregular operations and wage conventional campaigns.[10]

> The 21st Century began with 9/11, the subsequent Global War on Terrorism and operations in Iraq and Afghanistan. The Army recognized that it lacked the breadth and depth of capabilities required for this long, irregular war. The 2006 Quadrennial Defense Review and associated analysis present a defense strategy that includes traditional and also irregular, catastrophic and disruptive challenges. To mitigate risk, provide a broader portfolio of capabilities and to increase the options available to the President and combatant commanders the Army is transforming. The Army is increasing both its capability and its capacity by creating modular, multipurpose, brigade-based combat and support forces. The brigade-based forces are better able to operate as elements of joint, expeditionary force packages and to conduct sustained campaigns.[11]

The Army has programmed its long-term investments against this changing environment. Army's portion (Total Obligation Authority) of the President's 2007 budget is $110.4 billion.[12] The research, development, testing and procurement of information technologies by the Army will fall into two appropriations groupings: Research, Development, Test and Evaluation (RDT&E) and Procurement.

The Research, Development, Test and Evaluation appropriation provides funds for exploring and examining technologies into weapons systems, system upgrades and other products for the warfighter. The Army RDT&E budget for 2007 is $10.8 billion-$1.2 billion above the FY 2006 Presidental budget. The RDT&E budget for FY 2007 provides $3.7 billion, i.e. 34 percent of all RDT&E for Future Combat Systems (FCS) to continue the advance in new technologies and, when available, to spiral emerging capabilities for the warfighters. In addition to FCS, the FY 2007 budget allows the Army to move forward with delivery of the first iterations of the new Battle Command Control Network, Unattended Ground Sensors and Intelligent Munitions Systems and the Non-Line-of-Sight Launch System.[13] Key information technology RDT&E investments in FY 2007 include $158 million for Warfighter Information Network-Tactical (WIN-T), $832 million for Joint Tactical Radio System (JTRS), $38 million for Command, Control

& Communications (C3), $38 million for Maneuver Control, $26 for Force XXI Battle Command, Brigade and Below (FBCB2) and $41 million for Satellite Communication (SATCOM) Ground Environment.[14] All told there is $1.1 billion budgeted in the Army for RDT&E on tactical information systems technology in the FY 2007 budget.

The Army Procurement budget for FY 2007 is $16.8 billion--$1 billion above the FY 2006 proposal and $5 billion above the FY 2006 President's budget. The Army Procurement budget is 15 percent of the total Army budget and 20 percent of all DoD Procurement. The FY 2007 budget is approaching the levels of the FY 1990 budget from the end of the Cold War. A review of the Procurement funding since FY 1990 illustrates the post-Cold War reductions, the slow growth beginning in the late 1990s and the increases after 9/11 and for the GWOT.[15] All told there is $3.9 billion budgeted procurement (Other Procurement Army 2) for Communications & Electronic Equipment. One danger exists in that Army investments are not being matched by other services or potential coalition partners. How then will these Army modular forces be able to effectively interoperate in a joint and combined environment?

With these large Army investments being made in information systems technology research and procurement, the question now becomes what to do with all the information being provided to the tactical level. Recent experiences of forces deployed in the USCENTCOM theater of operations help to provide insight into the challenges facing tactical level commanders. One recent article (Sep/Oct 2006) in the Field Artillery Journal provides a view from the tactical edge.

> The process of receiving, assimilating, filtering and conveying relevant information to an individual is a challenge that every Army leader will experience. Over the course of many combat deployments, it becomes evident that the concept of too much or too little information can cost commanders their ability to make sound decisions. Outlining information and determining for the commander where the critical decisions must be made set the conditions for success. Leaders in a deployed unit make far more critical decisions than garrison leaders on a daily basis. Almost every decision a deployed leader makes has implications for accomplishing the mission and the providing for the well being of Soldiers. Too much information wastes time and clutters the decision-making process. Too little information causes the leader to either make the wrong decision due to ignorance or requires a request for more information, which wastes time at a critical moment. Too many units have gotten into the habit of overwhelming leaders with information, beating them into submission with nonessential details. Robust information systems technology allow for the leaders to see vast amounts of information, however a leader who focuses on everything, focuses on nothing.[16]

The experiences relayed from Army units in Iraq are not the only example cited. The 1st Marine Division identified similar misgivings as those presented by the Army.

> Every standard problem of bottleneck and overload in information emerged, and almost every "push" and "pull" technique to manage them failed. National intelligence sources were great for developing deep targets, subject to the prioritization of high Headquarters (Division and higher). Navigating the labyrinth of collection tasking processes proved too difficult in most cases to get reporting on Division targets; the problem was certainly ever more complex for Battalion-level collections. Communications within intelligence sections were better, but "at all levels they were inundated with information and data that had little bearing on the mission and Intelligence requirements".[17]

When talking about the potentials of remote sensor technologies, Vice ADM Herbert A. Browne, USN (Ret) provided the following comments:

> The military is on the cusp of a new generation of sensor advances. Signal processing and detection technologies are uniting to provide better information and understanding than ever before. Combine that with the global network being extended to the warfighter and you have potential for the greatest situational awareness picture ever envisioned by a military planner. However, the pitfall that the military must avoid has not changed: sensor overload. Information that is collected by a sensor must get to the person who needs it in the right format and in a timely manner. How to do that has been a topic of debate for years.[18]

Examples in the Air Force are also provided:

> In one case of friendly fire in Afghanistan during March 2002, information overload, friction between layers of command and inexperienced personnel swamped exactly those air forces and commands that fought in Iraq a year later. Data was so plentiful that USAF squadron commanders could not or did not circulate much of it from ATOs to their pilots, while staff officers would not change their procedures, thus ensuring confusion between all layers of command.[19]

Operation Iraq Freedom demonstrated a new standard for conventional war. ADM Cebrowski, Director, DoD Transformation, proclaimed "the discovery of a new 'sweet-spot' in the relationship between land and air warfare and a tighter integration of the two." The things that compel are good sensors networked with good intelligence disseminated through a robust networking system, which then yields speed. Speed turns out to be very, very important."[20]

> C4ISR, IO and NCW worked as planned, because Coalition forces had the initiative and followed their plan, while the enemy was passive, overwhelmed, unable to strike their forces or C4ISR. Had the Iraqis jammed GPS or tactical communication, they would have broken most of the Coalition's enhanced power in intelligence and precision attack; had they harmed satellites, strategic signal or computers, they would have crippled the Coalition's command. The sources of one's strength are one's vulnerability. How far this success can be repeated is unsure—NCW, C4ISR and IO worked less well in Kosovo; turkey shoots offer few lessons in tactics. So one-sided was this war that intelligence served primarily for target acquisition rather than ONA**.** Dust and heat in rooms housing SIPRnet servers and routers endangered C4ISR more than did the Iraqis. Could this near-NCW system work in complex operations against an able and

> aggressive enemy? In Afghanistan and Iraq, precision strikes often failed, showing they work only when the machine performs without friction. Any friction yields failure; no system can always be perfect. An enemy that fights by its own rules, like light infantry willing to die, or else silently to steal away, has caught American forces at a disadvantage.[21]

Herein lies one of my concerns. How significant a force enabler is information technology when the enemy plays by its own rules? How effective an enabler will those technologies be against an unconventional threat that does not lend itself to remote sensors or that can combat our technologies with relatively inexpensive means.

The 1st Marine Division noted that while American forces grasped enemy capabilities, we remained largely ignorant of the intentions of enemy commanders. This shortcoming was especially critical as much of the war plan was either based on or keyed to specific enemy responses. When the enemy "failed" to act in accordance with common military practices, we were caught flat footed. In trying to map out the opposition's reactions we were largely relegated to our OSINT sources and rank speculation based on our own perceptions of the battlefield to make our assessments. Our technical dominance has made us overly reliant on technical and quantifiable intelligence collection means. There is an institutional failure to account for the most critical dimension of the battlefield, the human one.[22]

> When considering the quality of the information being provided, one defense official offered the following: intelligence gatherers are tossing unfiltered information "over the transom" to the center in order to cover themselves in case an event does take place. This is creating a "fog of information." There is the risk of an "echo effect" where one piece of information on a possible terrorist attack goes out in a memo and it is suddenly repeated in a half-dozen other reports. The readers may believe there is a wealth of confirmation, when in fact, the intelligence is derived from only one source.[23]

This is an example of another of my concerns regarding broadly deployed robust information system technologies to the tactical level. This is the very problem that adds to the fog of war at the tactical level. Do the tactical units (brigade and below) have the means to separate fact from friction? Do they have the means to analyze for both relevance and accuracy the vast amounts of information available on the network? Will their inability to process this vast amount of information inhibit their ability to key in on the most critical information? As previously stated, information that is collected by a sensor must get to the person who needs it in the right format and in a timely manner.

Recent Israeli experiences during the 2006 Lebanon War caused some to ask the question: Does technology help or hinder the ability to command and control fighting forces? At the core of these so-called gaps between the conceptual and the concrete is leadership, which

may have suffered from a misplaced reliance on the potential-rather than practical-benefits of technology. Israel's first digitized ground war after-action probes found egregious cases where commanders relied on situational awareness provided by the sensor-fused data streaming into command centers instead of moving forward to assess critical points in the evolving battle.[24]

"This war underscored the limitations of plasma, especially when it is accorded disproportionate priority over training and discipline," said Matan Vilnai, a retied major general and former Israeli Defense Forces (IDF) deputy chief of staff. "Plasma" has become the derisive shorthand for virtual command and control provided through networked operations. Examples of such dangers were found in the wartime functioning of two critical divisions, where both brigadier general commanders were assailed for lack of hands-on contact with forces under their control.[25]

"Even though a commander may have excellent information coming in through the net, he still needs to go down into the field to get a clear understanding of reality in his sector," said Doron Almog, the retired IDF major general who led a post-conflict investigation into the causes for certain failures. He further states, "No pictures from unmanned aerial vehicles and no amount of plasma is going tell him how his people are interpreting and implementing orders, what are their concerns, and how is their state of morale. For that, you need to spend time with them, educate them and support them"[26] In this case, information technology may not have been the direct culprit, but it enabled the true cause. Poor leadership or ineffective troop leading procedures may become a common byproduct of information technically enabled forces in the future.

Lastly, I want to briefly discuss the impact on the human element of broadly deployed battlefield information technology. Individuals have a limit for processing data. Research indicates that, on the average, when an individual is working with more than approximately seven pieces of information, information overload will result.[27] Does this limitation translate well into the suite of technologies embedded inside brigade and battalion tactical operations centers (TOC) of today's force? A visit to any brigade or battalion TOC would indicate otherwise. What you will find inside the operations centers of today are a myriad of computer systems, plasma displays, projection screens, dry erase boards, and smart boards displaying blue force tracking, air tracks, unmanned aerial vehicle (UAV) tracks, UAV feeds, red force tracks, spot reports and CNN. Some old school commanders may still keep map boards, decision matrixes, daily CEOI information, and ever updated upcoming events. Add to this broad array of visual stimuli the many other factors influencing decision-making. Time, stress, fatigue, information demand, information overload, noise, and sleep deprivation, to mention some, are part of the warfare.

Therefore, today's battlefield decision-makers are confronted with so many distractions on their attention that it becomes difficult to focus in on key elements of information.

Martin Van Crevald argues that command can be viewed as both an organizational function and a cognitive function, and that technology by itself is not a panacea. There are two elements that present obstacles to certainty according to Van Crevald: nature and logic. Logic dictates that all information relevant to a decision must be obtained in order to achieve certainty as an outcome of that decision. This leads to a paradox in that the more information that is gathered, the longer it will take to process it. The result is a more confused situation where it becomes difficult to separate important, relevant, and reliable pieces of information from unimportant, irrelevant, and unreliable ones.[28]

The science of decision-making seeks certainty, rationality, and logic. It is articulate and analytic. The ability to take time to ruminate and contemplate, which may be required to deal with confusion and uncertainty, is becoming outdated. The computer in the command and control system cannot deal with confusion. The danger exists that subtler intended meanings might get lost during the process of articulating the material into something that "computes."[29]

In conclusion, I think it is important to review and understand the risks inherent in too broad of a dependence on information technologies within the force.

> Information technology's first vulnerability is that information systems can overwhelm commanders and staffs because of the "sheer volume of information available and the fact that much of it is conflicting or irrelevant 'noise.'" The ability of information systems to produce sheer volumes of information, accurate and inaccurate, relevant and irrelevant, is an inherent friction that puts a premium on a commander's ability to use his power of intellect including his ability to use judgment, intuition, and experience to understand and identify the relevant information he needs to make a decision.[30]

If commanders and their staffs learn to deal with the sheer volume of information on the network, then another risk emerges.

> The ability of network-centric operations to produce high volumes of information can cause commanders to become overly reliant on information technology. Relying too much on information technology can cause a commander to wait for all possible information in the hope he can make a risk-free decision. High volumes of information will always contain noise that will cause the friction and uncertainty that delay decision making. But the noise might also hide relevant information that might or might not be readily apparent or the one piece of information a commander is looking for might never come.[31]

As process changes are exercised to effectively deal with the volume, relevance and integrity of the information, then physical limitation may be a factor. Information technology and networks use sophisticated equipment and systems that can break or that adversaries can

attack.[32] These electronic systems are vulnerable to extremes in environmental conditions (e.g. heat, moisture) as well as susceptibility to dust and dirt. These systems require uninterrupted power, controlled temperatures, and filtered air in order to provide sustained availability. In addition to the physical and environmental vulnerabilities associated with information systems, networking devices and digital transport communications, many of these systems are a part of larger networks that are susceptible to intentional network attack and exploitation.

Having looked at all the risks from within our own doctrinal and organizational construct, there emerges perhaps the greatest risk of all.

> The presence of a thinking enemy and the psychological dimension of war contribute to an uncertainty that information technology cannot penetrate. For all its benefits, information technology does not enable our tactical leaders to see into the skull of our adversary. War is a violent conflict between adversaries trying to impose their will on each other where "the will is directed at an animate object that reacts." War contains killing and death; it is where a "struggle or interaction takes place in the psychological and emotional realms and effects fighting power on both sides and where uncertainty both derives from and reinforces the strains of war in ways that defy prediction." The psychology and human sides of war will always perpetrate uncertainty because they are hard to quantify and predict. The human and psychological dynamics of warfare also preserve uncertainty because a commander can only make an informed, educated guess about the enemy's plans and intent. Even during the battle or contact with the enemy it is still unclear what the enemy will do or how he will react.[33]

For all its benefits, information technology still possesses a significant limitation on the battlefield.

> Information technology and sensors might be able to provide a commander some locations and movements of enemy forces and the ability to share the information with subordinates. However, information systems cannot provide an adversary's intentions and plans. It does not show how an adversary plans to impose its will. The battle command quality that facilitates understanding enemy intentions is the ability to visualize the enemy through knowledge and training, part of personal and professional attributes, and intuition that Napoleon called "seeing the other side of the hill."[34]

Likewise, information technology provides a passive near real time means to query, track, post, report and review friendly unit locations, movement and equipment status. However, information technology does not provide insight into the morale of subordinate units, understanding of commander's intent, levels of readiness to achieve the task at hand nor the ability to see the terrain through the eyes of the soldiers who will be operating on it.

According to Thomas Czerwinski, we stand at the crossroads with regard to command and control. One road is marked "technology" and the other "Art." The way forward must be

plotted out for us by the forward projection of doctrine, constantly updated, to reflect both requirements and improvements in understanding. The question is which way to choose, and whether or not the military will be able to change its focus from technology and digitization of the command and control system to rely more on "art."[35]

Here in lies the crux of my concern. I understand the benefits of information technology with all its high speed data processing, near real time information transfer and seemingly endless data storage. Information technology is a force enabler. When used to further enable solid troop leading procedures, information technology should speed the ability of tactical commanders to effectively visualize elements within their operating environment. Information technology should not replace troop leading procedures, but rather it should augment the foundation built through collective training, leader development, organizational standing operating procedures and pre-combat checks and rehearsals

I am not anti-information technology, but rather I understand its limitations and vulnerabilities. Rapid access to vast amounts of near real time information may mean tactical leaders will leverage unfiltered, unconfirmed, or erroneous information when making time sensitive decisions. Dependence of external information sources may cause tactical leaders to inhibit or disregard information collection developed locally. Local filters will be used by tactical leaders in order to deal with information overload. If not managed effectively, these same filters may peel off essential information needed by decision makers. Tactical units (brigade and below) are not normally staffed to deal with the vast amounts of information available through the network; therefore, care must be taken at the operational and strategic levels to ensure the accuracy and currency of information stores. Tactical leaders must condition their staffs to quickly identify relevant information for use in the military decision making process. Solid troop leading procedures need to be exercised routinely to facilitate the continuation of operations when information systems fall prey to environmental or adversarial disruption.

So what are the answers to the questions posed earlier? When is enough information technology enough? When do we cross the point of diminishing return? At what point do information planners and program managers provide too much information access? There is no definitive answer. I do know that it is incumbent on tactical leaders to understand their information needs. Leaders at all levels need to tailor their information dissemination management processes to best utilize the information systems and access they have deployed. The Army, as an institution, needs to match its investment in technology development and procurement with a continued investment in growing leaders who are able to continually adapt

to an evolving information environment, thereby providing a balance between the art and science of military leadership and command.

Endnotes

[1] LTC Jared A. Kline, "A Blessing and A Curse: Communications as an Enabler to Micro-Management," USAWC, Carlisle Barracks, PA, 9 April 2000, pg 6.

[2] Ibid, pg 6.

[3] Akshay Joshi, "A Holistic View of the Revolution in Military Affairs (RMA)," *Strategic Analysis, A Monthly Journal of the IDSA*, February 1999, p. 3.

[4] Vice Admiral K. Cebrowski and John J. Garstka, "Network Centric Warfare: Its Origin and Furture," *US Naval War College Proceedings*, January 1998, pg 29.

[5] Akshay Joshi, "A Holistic View of the Revolution in Military Affairs (RMA)," Strategic Analysis, *A Monthly Journal of the IDSA*, February 1999, p. 3.

[6] Ibid, p.3.

[7] Ibid, p.4.

[8] Ibid.

[9] Ibid, p.7.

[10] Frank A. DiStasio, "Fiscal Year 2007 Army Budget, An Analysis," *The Institute of Land Warfare, Association of the United States Army*, 2006, p vii.

[11] Ibid, p. 50.

[12] Ibid, p. 45.

[13] Ibid, p.62.

[14] Ibid, pgs 65-67.

[15] Ibid, p.64.

[16] Timothy J. Doughtery and G. Damon Wells, "The Deployed Commander's Information Band of Tolerance," *FA Journal*, Fort Sill, Sep-Oct 2006, pgs 33-37.

[17] Ferris, John, "A New American Way of War? C4ISR in Operation Iraqi Freedom, A Provisional Assessment," Columbus International Affairs Online, Columbus University Press, June 2003, http://www.ciaonet.org/olj/jmss/jmss_2003/v6n1.pdf, pg. 6

[18] Herbert A. Browne, "Sensors and Sensibility," *Signal Magazine*, April 2006, p. 14.

[19] Major William A. Woodcock, “The Joint Forces Air Command Problem, Is Network-centric Warfare the Answer?” Naval *War College Review, Winter 2003*, p.46 the words are Woodcock’s, but his source is Michael Short, The Joint Force Commander in Kosovo.

[20] “What Went Right?” *Janes Defence Weekly*, 30.4.03.

[21] Ferris, John, “A New American Way of War? C4ISR in Operation Iraqi Freedom, A Provisional Assessment,” Columbus International Affairs Online, Columbus University Press, June 2003, http://www.ciaonet.org/olj/jmss/jmss_2003/v6n1.pdf, pg. 13.

[22] Ibid, p.3.

[23] Anonymous, “Information Overload,” *National Defense*, May 2006, Vol. 90, Iss 630; pg 9.

[24] Barbara Opall-Rome, “Does Technology Undercut War Leadership?”, *Defense News*, Nov 20, 2006, p.2.

[25] Ibid, p.3.

[26] Ibid.

[27] G.S. Miller, “The Magical Number Seven, Plus Two or Minus Two: Some Limits on our Capacilty for Processing Information,” *Psychological Review* (March 1956): pgs 81-97.

[28] Martin Van Crevald, “*Command in War*,” Cambridge, Mass., Harward University Press, 1985, p. 267.

[29] Guy Claxton, “*Hare Brain*, Tortoise Mind: How Intelligence Increases When You Think Less,” New York, NY, HarperCollins Publishers Inc, 1999, pgs 206-7.

[30] Demetrios J. Nicholson, “Seeing the other side of the Hill: The Art of Battle Command Decisionmaking, Uncertainty, and the Information Superiority Complex,” *Military Review*, Ft Leavenworth: Nov/Dec 2005. pg 62.

[31] Ibid. pg 61.

[32] Ibid.

[33] Ibid.

[34] Ibid.

[35] Rolf I. Roth, “The Rational Analytical Approach to Decision-Making: An Adequate Strategy for Military Commanders,” *The Quarterly Journal*, Vol. III, No.2, June 2004, p. 81.